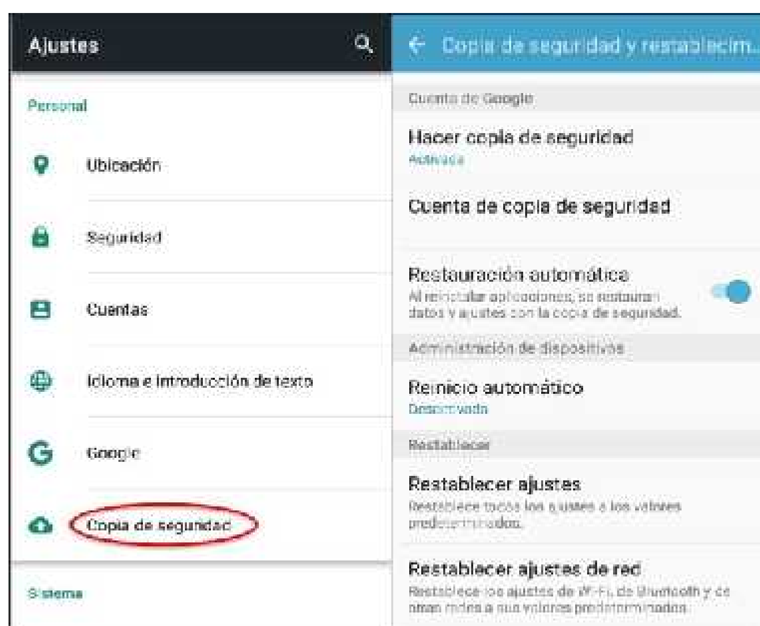
Guía Básica de Seguridad y Privacidad para dispositivos móviles con sistema Android.

<u>Consideración generales</u>:

Esta guía comprende orientaciones básicas y no tan complejas para configurar y manipular nuestro dispositivo móvil con mayor seguridad y privacidad de lo que nos ofrece la propia empresa de origen. Mencionar además que estas especificaciones fueron probadas en móviles con ROM de fábrica, con o sin *rootear*[1] y con Android versiones 4.2/4.4/6.0, año 2013, 2016 y 2017 (si tienes una versión anterior o más nueva es probable que los nombres de las opciones puedan cambiar o simplemente no aparezcan en su móvil, lo más probable en móviles de origen chino).

IMPORTANTE: recomiendo hacer un *backup* o copia de seguridad de todo su celular con app, con TWRP *Recovery*[2] o con la opción en "Ajustes" de "Copia de seguridad y restablecer/Hacer una copia de seguridad".



[1] Tener el control total y todos los privilegios o permisos necesarios para hacer y deshacer operaciones del celular.
[2] Team Win Recovery Project es una imagen de recuperación personalizada que instala, limpia, realiza copias, restaura copias y otras operaciones. (Es software de código abierto).

A.- Operaciones externas del dispositivo:

1.- Ocultar cámara frontal con adhesivo oscuro: Se recomienda huincha aisladora negra. Existen varias formas de prender la cámara de nuestro dispositivo de forma remota, utilizando programas que son *hack*, tanto para ordenadores como para dispositivos celulares.

En caso de querer ocultar el adhesivo, lo puedes hacer desarmando el celular hasta llegar a la placa y adherir, en un tamaño mucho menor, el adhesivo oscuro encima de la cámara frontal. Luego armas tu celular y no se verá el adhesivo externamente.



B.- Operaciones en el software del dispositivo:

Lo primero que haremos es considerar el **primer encendido del celular** luego que salió de la fábrica (celular nuevo), el cual corresponde a la primera configuración inicial del móvil para su primer uso, en que, por lo general, y dependiendo de la empresa del móvil, mostrara; "Registro del Móvil", es decir datos del propietario. "Cuenta Google", que es dar nuestro correo electrónico que usemos. Y por último la "Sincronización y Enviar Datos Estadísticos de Google". Los cuales se recomienda desmarcar o desactivar todas las opciones y seleccionar datos que no comprometan nuestra real identificación personal.

Si ya tienen la configuración inicial de su móvil con datos que no desean, pueden optar a "*flashear*[3]" su móvil, para volver a cero su dispositivo, como recién salido de fábrica (es parecido a un formateo a bajo nivel en ordenadores). Pero esta operación es compleja y delicada, y será descrita en otra guía.

Luego de la configuración del primer inicio, nos vamos a lo siguiente:

[3] En Android o iOS cuando dices *Flashear* te refieres a reinstalar el sistema operativo del aparato.



1.- Seleccionamos AJUSTES o CONFIGURACION, luego buscamos **BLUETOTH** y lo desactivamos, y en caso de haber historial de búsquedas las borramos.

2.- En AJUSTES o CONFIGURACION, vamos a **LAUNCHER** o **PAGINA PRINCIPAL**, la cual es la organización de los elementos de tu móvil (como un *theme* en Windows). Por defecto viene un *launcher*[4] de Google, Google Now, recomiendo que lo cambies por otro, que hay varios como Smart o Nova, que son más configurables en velocidad, privacidad y seguridad para tu móvil.

3.- En AJUSTES o CONFIGURACION, luego vamos a **APLICACIONES o ADMINISTRADOR DE APLICACIONES**, y luego a "Configurar Aplicaciones" o "Avanzada". Aquí nos aparecerán varias opciones, seleccionamos la primera:



[4] El *Launcher* es un programa o aplicación que permite cambiar determinadas características de la interfaz de usuario, puedes personalizar el dispositivo para adaptarlo a tu estilo con fondos de pantalla, colores del tema, paquetes de iconos y mucho más.

- PERMISOS DE APLICACIONES: y vamos por todas las opciones revisando las aplicaciones que tiene permisos y si queremos desactivar los permisos que tienen para acceder a información u operaciones de los sensores de nuestro móvil. Recomiendo revisar sobre todo Cámara, Micrófono, Sensores Corporales y Teléfono, y vayan desactivando las que consideren.

- MODIFICAR CONFIGURACION DEL SISTEMA: esta es otra opción en que ingresaremos y revisaremos cómo se comportan las aplicaciones instaladas, es decir, cuales son las que pueden o no modificar mi teléfono. Este apartado es un poco más sensible su modificación, pero lo dejo a criterio de ustedes.

Las demás opciones del apartado CONFIGURAR APLICACIONES lo dejamos tal cual.

4.- En AJUSTES o CONFIGURACION, vamos a **UBICACIÓN o GPS** y lo desactivamos. Además, abajo aparece un "Historial de ubicaciones de Google", la cual seleccionamos y borramos el historial.

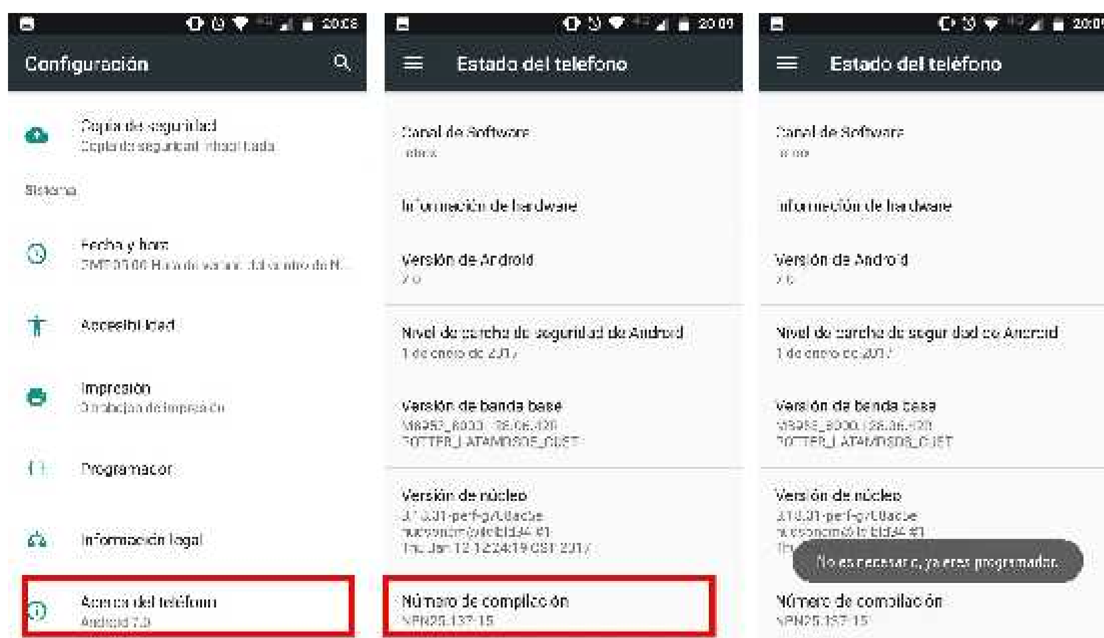


- Para los que no quieren dejar el GPS, pueden usarlo como *GPS Falso*, esto se hace activando "Opciones de Desarrollador" de Android e

instalando una aplicación *hack* (por ej: Fake GPS[5]). Y se realiza de la siguiente manera:



- CONFIGURACION o AJUSTES, “Acerca del Dispositivo”, “Número de Compilación”, le damos unas 6 o 7 veces hasta que aparezca “Eres programador”.



- Luego, volvemos y nos aparecerá otra nueva opción que se llama “Opción del programador”, la seleccionamos y activamos de momento solo las siguientes opciones: Depuración por USB luego y Ubicación de prueba. Esta última es la que nos interesa para el GPS Falso.

- En algunas versiones de Android aparecerá la opción “Elegir aplicación de ubicación de prueba”, la seleccionamos y ubicamos nuestra app de Fake GPS que tengamos previamente instalada.

[5] Aplicación que simula la ubicación GPS falsa de tu dispositivo.

- Configuramos la app y está listo.

- La otra forma de evadir nuestra ubicación, es cambiar la *dirección IP*[6] estática del celular, a una dinámica o estática de otro país. Esto lo explicare en otra guía.

5.- En AJUSTES o CONFIGURACION, y vamos a **SEGURIDAD**, luego en ADMIN. DE DISPOSITIVO, y aquí desactivamos "Encontrar mi dispositivo". Luego volvemos y activamos "Fuentes Desconocidas". Y por último vamos a "Acceso a Datos de Uso", y desactivamos las aplicaciones que consideremos peligrosas para que no puedan hacer seguimiento de lo que hacemos (en algunas versiones de Android esta opción aparece en "Datos de Uso").

- Recomiendo, además, en caso que les aparezca en "Seguridad", es de cifrar su dispositivo.

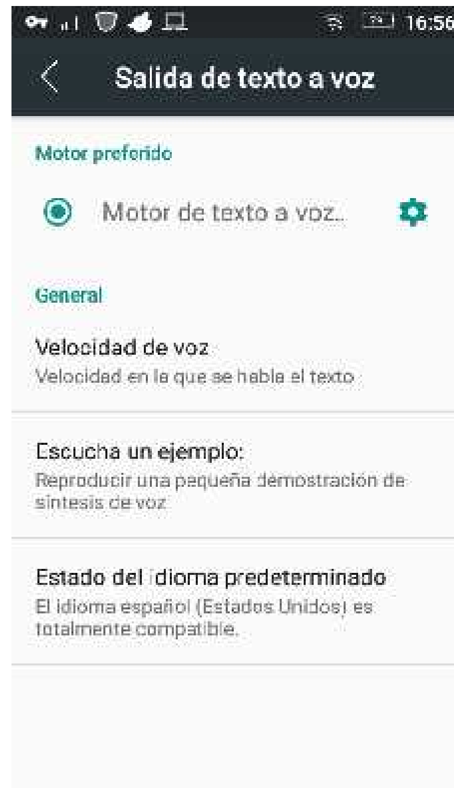


6.- En AJUSTES o CONFIGURACION, vamos a **TECLADO E IDIOMA**. Aquí recomiendo cambiar el teclado por defecto, ya que google graba toda nuestra información que tecleamos, aunque desactivemos esta opción desde las opciones de google. Hay varias apps de teclados más livianas y seguras

[6] Una dirección IP es un número que identifica, de manera lógica y jerárquica, a una Interfaz en red de un dispositivo (computadora, tableta, portátil, smartphone). Y con ese número IP se puede obtener identificación personal y ubicación del propietario del dispositivo.

(ej: MultiLing Keyboard, Smart Keyboard, etc., ambas las puedes encontrar en la Play Store y versiones de pago en Blackmart[7]).

Una vez cambiado el teclado y configuradas las opciones de la app keyboard, vamos a “Salida de Texto a Voz”, y vamos a la opción de “Motor de Texto a Voz”, luego en “Configuración de Motor de Texto a Voz” y desactivamos todo lo que aparece en ese apartado, sobre todo la opción “Informes Anónimos de Uso”.



7.- En AJUSTES o CONFIGURACION, luego en **ACCESIBILIDAD**, puedes ver en “Servicios” algunas aplicaciones que pueden acceder a servicios exclusivos de su celular. Recomiendo que revisen uno por uno y desactiven las que consideren.

8.- En AJUSTES o CONFIGURACION, bajamos al final en **ACERCA DEL DISPOSITIVO**, la única opción que veremos para desmarcar es “Participar en Experiencia *nombreempresa*”, desactivamos, ya que activada enviara información de nuestro uso a la empresa cada cierto tiempo. (En algunos

[7] Aplicación también conocida como Mercado Negro, en la que puedes descargar aplicaciones de pago como Pro, Premium o Mod Unlocked. Sugiero revisar esta aplicación con precaución por contener algunas aplicaciones virus.

celulares no aparece esta opción, solo cuando es encendido por primera vez).

9.- Nos vamos a la aplicación **GOOGLE o CONFIGURACION DE GOOGLE**, ahí seleccionamos las tres rayitas que están abajo en la esquina derecha y luego "Configuración" y en Notificación desactivamos todas las opciones, luego en Cuentas y Privacidad y luego en "Mi Actividad", y veremos todas las actividades que Google nos tiene registradas (los videos, las búsquedas, historial de ubicación, etc.). Bueno, para eliminar el historial vamos a los tres puntitos de arriba a la derecha y luego seleccionamos "Eliminar Actividad por", y luego colocamos "Eliminar por fecha Desde Siempre" y "Todos Los Productos", y luego seleccionamos "Eliminar".



Volvemos a "Cuentas y Privacidad", y seleccionamos "Controles de Actividad de Google", que nos enviara a una página web de google. Y nos aparecen una serie de opciones que estarán activas para ver, informar y utilizar nuestra información personal. Vamos desactivando una por una, y reingresamos a ese apartado nuevamente para revisar que estén desactivadas, ya que, que me ha sucedido en varios celulares que google reactiva las opciones automáticamente luego de los primeros 2 o 3 intentos. (Nota: esto también lo puedes hacer desde tu ordenador, entrando a la configuración de cuenta de tu correo electrónico).



- ✓ Actividad en la Web y en Aplicación: desmarcar “Incluye el historial de Chrome…”, y luego desactivar.
- ✓ Historial de ubicaciones: desactivar. Luego ir a “Administrar Actividad” y borrar historial.
- ✓ Información del dispositivo: desactivar.
- ✓ Actividad de voz y audio: desactivar.
- ✓ Historial de búsquedas de youtube: desactivar

- Volvemos a “Cuentas y privacidad”, y desactivamos “habilitar recientes”, “filtro de safe search” y “editar y compartir capturas”.

- Volvemos ahora a la pantalla principal de “Configuración de Google” y seleccionamos “Voz, y desactivamos todas las opciones.

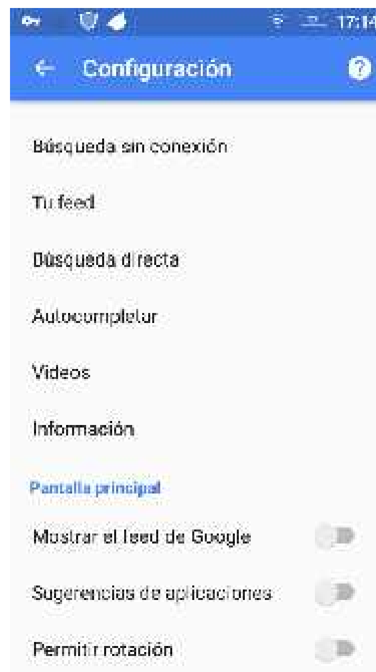
- Seleccionamos “Tu feed”, y también desmarcamos todo.

- Luego seleccionamos “Búsqueda directa”, desmarcamos todo.

- En “Autocompletar”, desmarcamos todo.

- En “Videos”, desmarcamos todo.

- Y, por último, en "Pantalla Principal", desmarcamos "Mostrar el feed de google", "Sugerencias de aplicaciones" y "Permitir rotación".



Una vez configurado este punto nº9, recomiendo "*congelar*" esta aplicación junto con el "Google Now" (habiendo cambiado previamente el launcher, sino ocasionara un error en su celular), con la app Titanium Backup Pro (además, pueden hacer un respaldo .zip completísimo de todo su celular, muy recomendada), que la pueden descargar en su versión completa desde la siguiente página: https://todoandroidvzla2.blogspot.com. Si desconocen cómo se realiza este paso, lo explicare en detalle en otra guía, ya que además debe estar rooteado su celular.



10.- Ahora, en este punto configuraremos la app “**Play Store**” (probada en versión 12.1.18). Haremos lo siguiente:



- Una vez iniciada la app “Play Store”, e ingresado nuestro correo electrónico, nos dirigimos a las tres líneas de la esquina superior izquierda, ahí seleccionamos “Play Project” y desactivamos, en este orden: “Detección de apps dañinas” y luego “Buscar amenazas de seguridad”.

- Volvemos, y seleccionamos “Configuración”, luego “Notificaciones” y desactivamos “Actualizaciones”, “Actualizaciones automáticas”, “Registro anticipado” y “Ofertas y promociones”.

- Volvemos, y seleccionamos “Actualizar aplicaciones automáticamente”, y seleccionamos “No actualizar apps automáticamente”.

- Volvemos, le damos a “Borrar historial de búsqueda local”.

- Volvemos, y seleccionamos “Controles parentales”, y lo desactivamos.

- Volvemos, y por último seleccionamos “Google Play Instant” y lo dejamos en “Ninguna”.

- En cuanto a las aplicaciones de fábrica que debemos desinstalar y otras que sugiero instalar, es un poco más complejo, por lo que estará especificado en otra guía.

11.- Habiendo realizado todas estas operaciones, reiniciarnos nuestro celular.

NOTAS DE CIERRE:

Todas estas operaciones están destinadas a la seguridad y privacidad de toda persona comunicadora independiente y organizaciones sociales de todo el mundo.

Es liberada su distribución sin incurrir en su venta, y en la responsabilidad de a quienes se ofrezca este material.

v1.1.